REMARKS

Reconsideration of the above application is requested.

Double Patenting

The examiner provisionally rejected claims 1, 4, 8-10, 13, and 16 under 35 U.S.C. 101 as claiming the same invention as that of claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of co-pending Application No. US 2002/0035683 A1, hereinafter '683.

In the alternative, the examiner provisionally rejected claims 1, 4, 8-10, 13, and 16 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of co-pending Application No. US 2002/0035683 A1, hereinafter '683. The examiner stated in part:

> **Although the conflicting claims are not identical, they are not patentably distinct from each other because, the monitoring devices and/or probe or plurality of probes devices are monitors that are statistical collectors in both applications. Similarly, the cluster heads are in fact the controllers/centers for the monitor/probes in both applications. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of US application '683, by labeling the cluster heads as controllers/centers, and the probe devices/monitors as statistical collectors/monitors as recited in the disclosure. One of ordinary skill in the art would have been motivated to perform such a modification because it involves only the aspect of labeling the functions of the device and not modifying its structure. One of ordinary skill in the art would have seen this as an obvious expedient to renaming the function of the device/apparatus/system, while retaining the original functions.**

Claims 1, 12, 28, as originally filed in the co-pending application '683 claimed:

> 1. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:
>
> monitoring network traffic through monitors disposed at a plurality of points in the network; and
>
> communicating data from the monitors, over a hardened, redundant network, to a central controller.

12. A distributed system to thwarting denial of service attacks comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data for performance of intelligent traffic analysis and filtering to identify malicious traffic and to eliminate the malicious traffic to thwart the denial of service attack.

28. A distributed system to thwart denial of service attacks comprises:

a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering identify malicious traffic at the source of an attack to eliminate the malicious traffic and thwart the denial of service attack.

Pending Claims 1, 12 and 18 of '683 recite:

1. A method of thwarting denial of service attacks on a victim data center coupled to a network, the method comprising:

monitoring network traffic through monitors disposed at a plurality of points in the network;

communicating data from the monitors to a central controller, over a redundant network[[,]] that is a different network from the network being monitored;

analyzing the data comprising network traffic statistics to identify network traffic that is part of a denial of service attack; and

filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as part of the denial of service attack.

12. A distributed system to thwarting denial of service attacks comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data for performance of intelligent traffic analysis and filtering to identify malicious traffic and to eliminate the malicious traffic to thwart the denial of service attack.

28. A distributed system to thwart denial of service attacks comprises:

a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering, identify malicious traffic at the source of an attack, to eliminate the malicious traffic and thwart the denial of service attack.

Claim 1 from the instant case recites:

1. A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a plurality of probe devices that are coupled to links that couple the network to the data center and collect statistical information on packets that are sent over the links that couple the network to the data center;

a cluster head coupled to each of the plurality of probe devices, the cluster head receiving collected statistical information from the probe devices and determining from the collected information whether the data center is under a denial of service attack.

8. (Currently Amended) A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through probes that are coupled to links between the victim data center and the network; and

communicating data from the probes, over a dedicated network, to a cluster head device.

9. (Original) The method of claim 8 further comprising:

communicating data from the cluster head device to a control center over a hardened network.

10. (Original) The method of claim 8 further comprising:

analyzing network traffic statistics to identify malicious network traffic; and

filtering network traffic, which is identified as malicious network traffic, during analyzing of the network traffic.

13. (Original) The method of claim 8 further comprising:

performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

15. (Currently Amended) A gateway for thwarting denial of service attacks on a victim data center comprises:

a cluster head; and

a plurality of probes disposed to monitor links that couple a network and a victim data center, the probes collecting statistical data, for performance of intelligent traffic analysis and filtering by the probes, to identify malicious traffic for thwarting denial of service attacks.

16. (Original) The gateway of claim 15 wherein the gateway includes a process to insert filters to discard packets that are deemed to be part of an attack.

101 Same type double patenting

In order for the examiner to establish that two claims claim the same invention within the meaning of 35 U.S.C. 101 the examiner must show that the same invention is being claimed twice. 35 U.S.C. 101 prevents two patents from issuing on the same invention. "Same invention" means identical subject matter. *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1984); *In re*

Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Ockert, 245 F.2d 467, 114 USPQ 330 (CCPA 1957).

It is clear from a comparison of claims 1, 3-4, 6-8, 12-15, 17, and 26-27 in the co-pending application '683 and the instant case that the same invention is not claimed twice. According to the MPEP

> **A reliable test for double patenting under 35 U.S.C. 101 is whether a claim in the application could be literally infringed without literally infringing a corresponding claim in the patent. In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970). Is there an embodiment of the invention that falls within the scope of one claim, but not the other? If there is such an embodiment, then identical subject matter is not defined by both claims and statutory double patenting would not exist. For example, the invention defined by a claim reciting a compound having a "halogen" substituent is not identical to or substantively the same as a claim reciting the same compound except having a "chlorine" substituent in place of the halogen because "halogen" is broader than "chlorine." On the other hand, claims may be differently worded and still define the same invention. Thus, a claim reciting a widget having a length of "36 inches" defines the same invention as a claim reciting the same widget having a length of "3 feet."**

Claim 1 of the instant case does not claim the same invention of claim 1 of the '683 co-pending application. Claim 1 of the instant case has two structural elements, whereas claim 1 of the'683 application has four method actions. Claim 1 of the instant case also does not claim the same invention as claim 12 or claim 28 of the co-pending application. Claim 12 of the co-pending application claims "a plurality of monitors dispersed throughout a network ... " whereas claim 1 of the instant case requires "a plurality of probe devices that are disposed to coupled to links that couple the network to the data center ... and a cluster head coupled to each of the plurality of probe devices. Claim 28 of the co-pending application claims "a plurality of gateways dispersed throughout a network ... ," but does not claim the "a plurality of probe devices that are disposed to coupled to links that couple the network to the data center ... and a cluster head.

None of the dependent claims of claims from the co-pending application recite "a plurality of probe devices that are disposed to coupled to links that couple the network to the data center ... and a cluster head coupled to each of the plurality of probe devices." Therefore no combination of the claims in the co-pending application can sustain a 101 statutory double

patenting rejection of claim 1 and its dependent claims, since in no instance is the same invention being claimed twice.

Claim 8 of the instant case has two method actions as does claim 9. Claim 10 of the instant case depends on claim 8 and with claim 8 has four method actions. However, claim 10 requires (from base claim 8, as amended) "monitoring network traffic through probes that are coupled to links between the victim data center and the network." At least this feature of monitoring through probes that are coupled over links between the victim data center and network and the feature of communicating data from the probes, over a dedicated network, to a cluster head device are not present in claims 1, 3-4, 6-8, 12-15, 17, and 26-27 or the other claims of co-pending Application '683. Inherently, the claims of '683 do not claim the same invention nor literally infringe the claims of the subject application. Therefore, this rejection is improper and should be removed.

None of the dependent claims from claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of the co-pending application recite "monitoring network traffic through probes that are coupled to links between the victim data center and the network." Therefore no combination of the claims in the co-pending application can sustain a 101 statutory double patenting rejection of claim 8 and its dependent claims, since in no instance is the same invention being claimed twice.

Claim 15 of the instant case does not claim the same invention as claim 28 of the co-pending application. Claim 15 of the instant case calls for: "A gateway for thwarting denial of service attacks on a victim data center. Claim 15 includes the features of a cluster head and a plurality of probes disposed to monitor links that couple a network and a victim data center, the probes collecting statistical data, for performance of intelligent traffic analysis and filtering by the probes, to identify malicious traffic for thwarting denial of service attacks. In contrast, claim 28 of the co-pending application claims: "A distributed system to thwart denial of service attacks" that includes "a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering, identify malicious traffic at the source of an attack, to eliminate the malicious traffic and thwart the denial of service attack." Thus claims 15 and 28 do

not claim the same invention, claim 15 recites a gateway, whereas claim 28 requires plural gateways. In addition, Claim 15 requires the gateway to have a defined structure as a cluster head and a plurality of probes disposed to monitor links that couple a network and a victim data center. In contrast Claim 2 requires "a plurality of gateways dispersed throughout a network, near data centers." Claim 28 has no such requirement of a cluster head and a plurality of probes disposed to monitor links.

None of the dependent claims from claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of the co-pending application recite "a cluster head and a plurality of probes disposed to monitor links that couple a network and a victim data center." Therefore no combination of the claims in the co-pending application can sustain a 101 statutory double patenting rejection of claim 15 and its dependent claims, since in no instance is the same invention being claimed twice.

Obvious Type Double Patenting

In the examiner's Response to Arguments, the examiner takes the position that the features which Applicant urges that '683 does not teach, such as a cluster head, and the links from victim center and the network, etc are mere a "naming convention."

The examiner also mentions that the cluster head feature is only a black box in Applicant's specification. Again Applicant disagrees. The cluster head functions are clearly disclosed in the specification. While applicant does not need to claim all of these features, the cluster head is more than a mere black box and possesses features distinct from the control center described in the instant case and the co-pending application '683. Applicant contends now and as of record that not only do claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of the co-pending application fail to describe the cluster head, but these claims 1, 3-4, 6-8, 12-15, 17, and 26-27 also fail to describe or suggest the plurality of probe devices and the relation of the probe devices to monitoring of links between the victim data center and the network and the relation of those probes to the cluster head.

Therefore, Applicant disagrees with this rejection for the reasons of record. However, in order to advance prosecution, Applicant will consider submission of a terminal disclaimer upon removal by the examiner of the 101 statutory double patenting rejection and an indication of

allowance of the claimed subject matter in order to obviate the obvious type double patenting rejection.

Therefore, an indication of allowable claims in the application is in order, since the obviousness type double patenting rejection will be overcome at least by the proposed terminal disclaimer and the same type double patenting rejection is improper. There being no other rejections in the application, an indication of allowance is in order and such action is requested.

Enclosed is a **$225** check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 4/26/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21305456.doc